This document is scheduled to be published in the
Federal Register on 10/26/2023 and available online at
https://federalregister.gov/d/2023-23668, and on **https://govinfo.gov**

9110-9P

DEPARTMENT OF HOMELAND SECURITY

[CISA-2023-0026]

Request for Comment on Software Identification Ecosystem Option Analysis

AGENCY: Cybersecurity and Infrastructure Security Agency, Department of Homeland Security.

ACTION: Notice; Request for information.

SUMMARY: The Cybersecurity and Infrastructure Security Agency (CISA) announces the publication of "Software Identification Ecosystem Option Analysis," which is a white paper on software identification ecosystems and requests public comment on the paths forward identified by the paper and on the analysis of the merits and challenges of the software identifier ecosystems discussed. Additionally, CISA requests input on analysis or approaches currently absent from the paper.

DATES: Written comments are requested on or before **[INSERT DATE *45 DAYS* AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]**. Submissions received after that date may not be considered.

ADDRESSES: You may send comments, identified by CISA-2023-0026, by any of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the instructions for sending comments.

Instructions: All submissions received must include the words "Cybersecurity and Infrastructure Security Agency" and the docket number for this action. Comments received will be posted without alteration at http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket and comments received, please go to www.regulations.gov and enter docket number CISA-2023-0026.

To submit comments electronically:

1. Go to *www.regulations.gov*, and enter CISA-2023-0026 in the search field,

2. Click the “Comment Now!” icon, complete the required fields, and

3. Enter or attach your comments.

All submissions, including attachments and other supporting materials, will become part of the public record and may be subject to public disclosure. CISA reserves the right to publish relevant comments publicly, unedited and in their entirety. Do not include personal information, such as account numbers or Social Security numbers, or names of other individuals. Do not submit confidential business information or otherwise sensitive or protected information. All comments received will be posted to *http://www.regulations.gov*. Commenters are encouraged to identify the number of the specific topic or topics that they are addressing.

Commenters may access the “Software Identification Ecosystem Option Analysis” white paper on CISA’s website at: https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis.

FOR FURTHER INFORMATION CONTACT: Allan Friedman, 202-961-4349, sbom@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION:

I. Public Participation

Interested persons are invited to comment on this notice by submitting written data, views, or arguments using the method identified in the **ADDRESSES** section. All members of the public, including, but not limited to, specialists in the field, academic experts, industry, public interest groups, and those with relevant economic expertise, are invited to comment.

II. Background

Software identification is a key facilitator of effective vulnerability management. Software identifiers are labels for specific versions of software that conform to a defined format. An identifier enables users to track software in relation to other information, such as known vulnerabilities, mitigations for vulnerabilities, lists of approved or disallowed software, and adversary activities. An effective, harmonized software identification ecosystem will facilitate greater automation, inventory visibility, and broader, more effective use of software bills of materials (SBOMs).

The two key requirements for an effective software identification ecosystem are:

1. Timely availability of software identifiers across all software items; and
2. Software identifiers that support both precise identification and grouping of software items.

Key challenges for an effective software identification ecosystem are: (1) uniformly and deterministically generating or locating the identifier for an unknown piece of software (discoverability); (2) distributing unique identifiers for software such that one identifier is not associated with multiple software or versions (precision); and (3) developing a mechanism by which software versions are associated with each other (grouping).

The white paper evaluates the following key criteria for a successful software identifier format:

1. Identifiers all refer to a single variant of a given piece of software and support grouping expressions.
2. Identifiers are built to express a fine level of granularity with support for complete identifier enumeration.

Three software identifier formats are starting points, based on their current use and future potential:

Common Platform Enumeration (CPE): In a system based on CPE, a set of parties generate the software identifiers for the community. Each identifier is generated at a point in time and then distributed to the community.

Package URLs (purl): In a system based on purl, any number of parties may generate software identifiers for the community. purl's existing mechanisms for distributed identification generation also make it feasible as the foundation for a system with a searchable database, however its lack of uniformity presents challenges.

OmniBOR: In a system built on OmniBOR, any party is able to derive a software's identifier from an instance of a piece of software. These identifiers are mechanically generated based on inherent properties of a piece of software, which are available to anyone who has that piece of software. In some cases, these identifiers also contain information about the composition of the software, enabling further identification of its components.

The white paper identifies six paths forward for a software identification ecosystem. Although the paths are individually evaluated, they are not mutually exclusive as a solution.

1. Any party can generate a software's identifier. Inherent identifiers are used.
2. Many parties generate software identifiers. The generators then push the software identifiers to the community through the distribution of the software. Defined software identifiers are used.
3. A central authority oversees and supports the many parties who generate and distribute software identifiers. Defined software identifiers are used.
4. An active management system other than a central authority oversees and supports the many parties that generate inherent identifiers. Defined identifiers are used.
5. In addition to a defined identifier scheme (Paths 2, 3, and 4) there is a standardized structure to characterize unknown software. Correlation is done using fuzzy-matching over the set of provided characteristics.
6. Many parties use multiple defined identifier formats to generate software identifiers.

The "Software Identification Ecosystem Option Analysis" white paper identifies paths forward in solving the problem of software identification and explores the benefits and challenges of the various approaches, as well as the community or authority structure that would be needed to develop and sustain the identifier format ecosystem. In doing so, the white paper outlines the requirements and activities necessary to establish a harmonized software identification ecosystem to facilitate greater automation, inventory visibility, and the multi-faceted value proposition of broad adoption of Software Bill of Materials (SBOM).

III. List of Topics for Commenters

Commenters may access the “Software Identification Ecosystem Option Analysis” white paper on CISA’s website at: https://www.cisa.gov/resources-tools/resources/software-identification-ecosystem-option-analysis. CISA seeks comments on the following topics:

(1) Key requirements for an effective software identification ecosystem

(2) Merits and challenges of available software identifier formats

(3) The viability of a system reliant on inherent identifiers or defined identifiers

(4) The necessity of a central authority or other active managing body for a software identifier ecosystem

(5) Methodology for division of software identification responsibilities in an ecosystem where multiple software identifier formats are used

(6) Preferred paths forward

(7) Issues, challenges, or use cases not considered or addressed in the paper

(8) Stakeholders that should be included in deliberation

This notice is issued under the authority of 6 U.S.C. 652 and 659.

Eric Goldstein,
Executive Assistant Director,
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security.

[FR Doc. 2023-23668 Filed: 10/25/2023 8:45 am; Publication Date: 10/26/2023]